Lietuvos matematikos rinkinys
Lietuvos matematikų draugijos darbai, ser. B
55 t., 2014, 23–27

ISSN 0132-2818
www.mii.lt/LMR/

protokolas

Albertas Dvirnas

Kauno technologijos universitetas, Matematikos ir gamtos mokslų fakultetas
Studentų g. 50, LT-51368 Kaunas
E. paštas: albertas.dvirnas@ktu.lt

Santrauka. Šiame straipsnyje pateikiame rakto apsikeitimo protokolo, paremto dekompozijos uždaviniu nekomutatyvioms grupėms, pritaikymą Veilio algebroms. Tuo tikslu įrodome vieną Veilio algebros savybę, susijusią su centralizatoriumi. Be to, pateikiame rakto apsikeitimo aprašą bei pavyzdį Veilio algebrai bei Veilio algebrai su papildomais sąryšiais.

Raktiniai žodžiai: Veilio algebra, centralizatorius, rakto apsikeitimo protokolas.

Įvadas

Veilio algebra yra baigtinai generuota (turi baigtinį sudaromųjų skaičių), tačiau begalinės dimensijos. Be to, pirmoji Veilio algebra yra kvadratinio augimo, todėl atrodo, kad ji yra perspektyvus pasirinkimas kaip platforma Shpilrain–Ushakov rakto apsikeitimo protokolui [2].

Veilio algebra virš teigiamos charakteristikos lauko turi didelį centrą, todėl ir kiekvieno algebros elemento centralizatoriai yra dideli. Be to, Veilio algebros elementai turi nesudėtingai apskaičiuojamas kanonines formas, kurias galima realizuoti kompiuteriu. Šiame straipsnyje pateikiame Veilio algebros savybę, kuri padeda surasti tokį Veilio algebros poalgebrį, kurio elementai komutuotų su pasirinktu elementu.

Panaudodami tokį Veilio algebros poalgebrį, Veilio algebrą pritaikome Shpilrain–Ushakov rakto apsikeitimo protokolui.

1 Apibrėžimai ir pagalbinės sąvokos

1.1 Algebriniai apibrėžimai

1 apibrėžimas. Tegu k – žiedas, o $\{x_i,\ i \in I\}$ ($I \subset N$ – indeksų aibė) – nepriklausomų, nekomutuojančių sudaromųjų sistema virš k. Tada laisvasis k-žiedas, generuojamas sudaromųjų $\{x_i,\ i \in I\}$, žymimas

$$R = k\langle x_i;\ i \in I\rangle.$$

2 apibrėžimas. Jeigu $\{x_i,\ i \in I\}$ – komutuojančių sudaromųjų sistema virš k, tada laisvasis k-žiedas, generuojamas sudaromųjų $\{x_i,\ i \in I\}$, žymimas

$$R = k[x_i;\ i \in I].$$

3 apibrėžimas. Bet kuriems dviems elementams $x, y \in A$, čia A – bet kokia algebra, Li skliausteliais žymime

$$[x, y] := xy - yx. \tag{1}$$

4 apibrėžimas. Jeigu $R = k\langle x, y\rangle$, ir $F = \{yx - xy - 1\}$, tai $A_1(k) = R/(F)$ vadiname pirmąja Veilio algebra virš k.

Čia k žymime lauką, kurio charakteristika $char(k) = p$.

5 apibrėžimas. Algebros A centru vadiname aibę $Z(A)$, apibrėžiamą kaip

$$Z(A) := \big\{v \in A \mid [w, v] = 0,\ \forall w \in A\big\}. \tag{2}$$

6 apibrėžimas. Elemento $v \in A$ centralizatoriumi vadiname aibę $C(v)$, apibrėžiamą kaip

$$C(v) := \big\{w \in A \mid [w, v] = 0,\ w \in A\big\} \tag{3}$$

1.2 Veilio algebros savybės

1 teorema. *Pirmoji Veilio algebra $A_1(k)$ tenkina šias savybes* [3]:

1. $[y, x^n] = nx^{n-1}$, $n = 1, 2, \ldots$;
2. $[y^n, x] = ny^{n-1}$, $n = 1, 2, \ldots$;
3. $Z(A_1(k)) = k[x^p, y^p]$, *t. y. algebros centras yra laisvasis k-žiedas, generuojamas dviejų sudaromųjų* x^p, y^p;
4. *Veilio algebros $A_1(k)$ elementų normalioji (kanoninė) forma yra*

$$W = \sum_{i,j=0}^{\infty} a_{ij} x^i y^j, \quad a_{ij} \in k;$$

5. *Tegu $char(k) = p > 0$, $f(x, y), g(x, y) \in A_1(k)$. Tada daugybą $f(x, y) \cdot g(x, y)$ galime atlikti naudodami formulę*

$$f(x, y) \cdot g(x, y) = \sum_{k=0}^{p-1} \frac{1}{k!} \partial_y^k f(x, y) * \partial_x^k g(x, y),$$

čia $\partial_y^k f(x, y)$, $\partial_x^k g(x, y)$ yra algebros elementų $f(x, y)$ bei $g(x, y)$ k-tos eilės dalinės išvestinės atitinkamai y ir x atžvilgiu. Daugyba $*$ apibrėžiama kaip įprasta daugyba kartu su papildomu sąryšiu polinomams $[y, x] = 0$.

Įrodymas. Pavyzdžiui, pirmosios savybės įrodymas:

$$\begin{aligned}[y, x^n] &= y \cdot x^n - x^n \cdot y = y \cdot x^{n-1} \cdot x - x^{n-1} \cdot y \cdot x + x^{n-1} \cdot y \cdot x - x^{n-1} \cdot x \cdot y \\ &= [y, x^{n-1}]x + x^{n-1} = (n-1)x^{n-1} + x^{n-1} = nx^{n-1}. \qquad \square\end{aligned}$$

1.3 Shpilrain–Ushakov rakto apsikeitimo protokolas

7 apibrėžimas. Dekompozicijos uždavinio formuluotė: turint du elementus a, b iš algebros A ir du poalgebrius $V, W \subseteq A$, rasti elementus $v \in V$ ir $w \in W$, tokius, kad $b = vaw$.

Pasiremiant tuo, kad $vw = wv$ kiekvienam $v \in V$, $w \in W$, rakto apsikeitimo protokolas apibrėžiamas tokiu būdu:

1. Aldona pasirenka $a_1, a_2 \in V$ (privatus Aldonos raktas) ir siunčia $a_1 a a_2$ Broniui;
2. Bronius pasirenka $b_1, b_2 \in W$ (privatus Broniaus raktas) ir siunčia $b_1 a b_2$ Aldonai;
3. Aldona apskaičiuoja $K_V = a_1 b_1 a b_2 a_2$;
4. Bronius apskaičiuoja $K_W = b_1 a_1 a a_2 b_2$.

Kadangi $a_1 b_1 = b_1 a_1$ ir $b_2 a_2 = a_2 b_2$, tai $K_V = K_W$, todėl Adona bei Bronius turi bendrą privatų raktą.

2 Pagrindiniai rezultatai

2.1 Centralizatoriaus savybė

1 teiginys. *Tegu k – teigiamos charakteristikos laukas, $char(k) = p > 0$. Fiksuojamas elementas $a \in A_1(k)$. Tada*

$$Z\big(A_1(k)\big)[a] \subseteq C(a), \tag{4}$$

čia $Z(A_1(k))[a]$ yra polinomų žiedas virš $Z(A_1(k))$, generuojamas sudaromosios a.

Įrodymas. Tegu $H \in Z(A_1(k))[a]$. Tada H turi išraišką $H = \sum_i c_i a^i$, čia $c_i \in Z(A_1(k))$.

Tada, skaičiuojant tiesiogiai

$$\begin{aligned}[H, a] = Ha - aH = \sum_i c_i a^i a - a \sum_i c_i a^i \overset{c_i \in Z(A_1(k))}{=} \\ = \sum_i c_i a^{i+1} - \sum_i c_i a^{i+1} = \sum_i c_i \big(a^{i+1} - a^{i+1}\big) = 0.\end{aligned}$$

Taigi, $H \in C(a)$, todėl $Z(A_1(k))[a] \subseteq C(a)$. □

2.2 Pritaikymas rakto apsikeitimo protokolui

Čia paaiškiname, kaip Veilio algebrą galime pritaikyti kaip platformą Shpilrain–Ushakov rakto apsikeitimo protokolui:

2.2.1 Schema

Pasirenkame atsitiktinį $u \in A_1(k)$.

1. Aldona pasirenka $a_1 \in A_1(k)$ (privatus Aldonos raktas), ir siunčia atsitiktinį $v \in Z(A_1(k))[a_1]$ Broniui;

2. Bronius pasirenka $b_2 \in A_1(k)$ (privatus Broniaus raktas), ir siunčia atsitiktinį $w \in Z(A_1(k))[b_2]$ Aldonai;
3. Aldona pasirenka $a_2 \in Z(A_1(k))[w]$, Bronius pasirenka $b_1 \in Z(A_1(k))[v]$;
4. Aldona siunčia $a_1 u a_2$ Broniui;
5. Bronius siunčia $b_1 u b_2$ Aldonai;
6. Aldona apskaičiuoja $K_A = a_1 b_1 u b_2 a_2$;
7. Bronius apskaičiuoja $K_B = b_1 a_1 u a_2 b_2$.

Galiausiai,

$$K_A = a_1 b_1 u b_2 a_2 = b_1 a_1 u a_2 b_2 = K_B. \tag{5}$$

2.2.2 Pavyzdys

Pateiksime pavyzdį, kai $char(k) = p = 3$.

Pasirenkame atsitiktinį $u = \mathrm{Dx} + 2x$.

1. Aldona pasirenka $a_1 = (x+1)\mathrm{Dx} + x$ (privatus), ir siunčia atsitiktinį $v = (2x+2)\mathrm{Dx} + 2x + 1$ Broniui;
2. Bronius pasirenka $b_2 = 2x^3\mathrm{Dx} + 2$ (privatus), ir siunčia atsitiktinį $w = x^3\mathrm{Dx} + 2$ Aldonai;
3. Aldona pasirenka $a_2 = x^3\mathrm{Dx} + 1$, Bronius pasirenka $b_1 = (x+1)\mathrm{Dx} + x + 1$;
4. Aldona siunčia $a_1 u a_2 = (x^4 + x^3)\mathrm{Dx}^3 + (2x^5 + x + 1)\mathrm{Dx}^2 + (2x^5 + 2x^4 + 2x^3 + 2x^2)\mathrm{Dx} + 2x^2 + 2x + 2$ Broniui;
5. Bronius siunčia $b_1 u b_2 = (2x^4 + 2x^3)\mathrm{Dx}^3 + (x^5 + 2x^3 + 2x + 2)\mathrm{Dx}^2 + (x^5 + 2x^4 + x^3 + x^2 + 2)\mathrm{Dx} + x^2 + 2x + 1$ Aldonai;
6. Aldona apskaičiuoja $K_A = a_1 b_1 u b_2 a_2 = (2x^8 + x^7 + 2x^6)\mathrm{Dx}^5 + (x^9 + x^6 + x^5 + 2x^4 + x^3)\mathrm{Dx}^4 + (2x^9 + 2x^8 + x^7 + 2x^3 + 2x^2 + x + 2)\mathrm{Dx}^3 + (x^9 + x^8 + 2x^7 + x^5 + 2x^4 + 1)\mathrm{Dx}^2 + (2x^6 + 2x^5 + x^4 + 2x^2 + x + 1)\mathrm{Dx} + x^3 + x^2 + 2x + 2$;
7. Bronius apskaičiuoja $K_B = (2x^8 + x^7 + 2x^6)\mathrm{Dx}^5 + (x^9 + x^6 + x^5 + 2x^4 + x^3)\mathrm{Dx}^4 + (2x^9 + 2x^8 + x^7 + 2x^3 + 2x^2 + x + 2)\mathrm{Dx}^3 + (x^9 + x^8 + 2x^7 + x^5 + 2x^4 + 1)\mathrm{Dx}^2 + (2x^6 + 2x^5 + x^4 + 2x^2 + x + 1)\mathrm{Dx} + x^3 + x^2 + 2x + 2$.

Matome, kad iš tikrųjų $K_A = K_B$.

2.2.3 Pavyzdys su papildomais sąryšiais

Pateiksime pavyzdį, kai skaičiavimų supaprastinimui dar įvedami papildomi sąryšiai $x^3 = 1$, $y^3 = 1$, be to, $char(k) = p = 3$.

Pasirenkame atsitiktinį $u = (2x^2 + x + 1)\mathrm{Dx}^2 + (2x^2 + 2x)\mathrm{Dx} + 2x + 1$.

1. Aldona pasirenka $a_1 = x^2\mathrm{Dx}^2 + (2x^2 + x)\mathrm{Dx} + 2x + 2$ (privatus), ir siunčia atsitiktinį $v = 2x^2\mathrm{Dx}^2 + (x^2 + 2x)\mathrm{Dx} + x + 1$ Broniui;
2. Bronius pasirenka $b_2 = 2x^2\mathrm{Dx}^2 + \mathrm{Dx} + x^2 + x + 2$ (privatus), ir siunčia atsitiktinį $w = (2x^2 + x + 1)\mathrm{Dx}^2 + 2x^2 + 2x + 1$ Aldonai;
3. Aldona pasirenka $a_2 = x^2\mathrm{Dx}^2 + 2\mathrm{Dx} + 2x^2 + 2x$, Bronius pasirenka $b_1 = x^2\mathrm{Dx}^2 + (2x^2 + x)\mathrm{Dx} + 2x + 2$;
4. Aldona siunčia $a_1 u a_2 = (2x^2 + x + 1)\mathrm{Dx} + 2x^2 + 2x + 1$ Broniui;
5. Bronius siunčia $b_1 u b_2 = x^2\mathrm{Dx}^2 + (2x^2 + 2x)\mathrm{Dx} + x + 1$ Aldonai;

6. Aldona apskaičiuoja $K_A = a_1 b_1 u b_2 a_2 = (x^2+x+1)\mathrm{Dx}^2 + (x^2+2x)\mathrm{Dx} + x^2 + 1$;
7. Bronius apskaičiuoja $K_B = (x^2+x+1)\mathrm{Dx}^2 + (x^2+2x)\mathrm{Dx} + x^2 + 1$.

Matome, kad iš tikrųjų $K_A = K_B$.

2.2.4 Saugumas

Veilio algebra yra begalinės dimensijos, todėl neįmanoma sukurti tikros reprezentacijos į baigtinės eilės matricų algebrą su koeficientais iš lauko k, todėl matricų reprezentacijos ataka šiai Špilraino–Ušakovo protokolo realizacijai yra sunki, kai neįvedame papildomų sąryšių. Įvedus papildomus sąryšius, atsiranda tikros reprezentacijos.

Be to, kadangi Veilio algebra yra begalinės dimensijos, galime teigti, kad pasiūlytas metodas yra atsparus „ilgio atakai", kurią galima atlikti kai kuriems kasų grupių kriptosistemoms, pavyzdžiui, Birman–Ko–Lee metodui [1].

3 Išvados

Veilio algebrų taikymas atrodo perspektyvi nekomutatyvios kriptografijos kryptis, jau pritaikyta ir Grobnerio bazėms.

Ilgio ataka atrodo neefektyvi, nes, iš vienos pusės, Shpilrain–Ushakov protokolas pats yra saugus nuo šios atakos, antra, Veilio algebros augimas yra tik kvadratinis.

Literatūra

[1] J. Hughes and A. Tannenbaum. Length-based attacks for certain group based encryption rewriting systems. *CoRR*, 2003.

[2] V. Shpilrain and A. Ushakov. *A New Key Exchange Protocol Based on the Decomposition Problem, vol. 418.* American Mathematical Society, Providence, RI, 1999, 2006.

[3] Y. Tsuchimoto. Preliminaries on dixmier conjecture. *Mem. Fac. Sci. Kochi Univ. Ser. A Math.*, **24**:43–59, 2003.

SUMMARY

Weyl algebra based key exchange protocol
A. Dvirnas

In this article we introduce the Weyl algebras as a platform algebra for a key exchange protocol based on the decomposition problem. In order to use it as a platform, we prove one propery of the Weyl algebra, related to it's centralizer. Furthermore, we provide a scheme for the protocol and examples for the Weyl algebra and for the Weyl algebra with additional relations.

Keywords: Weyl Algebra, centralizer, key exchange protocol.